Strengthen Your Password Security

INTRO

Passwords are the first line of defense against cyber threats. Strong and unique passwords help protect your personal and organizations sensitive information. Follow these following these next steps to ensure robust security

Creating strong passwords

- Use at least 12 characters.
- Include a mix of uppercase letters, lowercase letters, numbers, and special characters.
- Avoid using common words, phrases, or easily guessable information
- Consider using a passphrase—a sequence of random words (e.g., "Correct-Horse-Battery-Staple").

Managing Passwords

- Use a password manager to generate and store strong, unique passwords.
- Do not reuse passwords across different accounts or services.
- Change your passwords regularly, especially if you suspect a breach.

Implement 2FA

- 2FA adds an extra layer of security by requiring a second form of verification.
- Use an authentication app rather than SMS for more security.
- Set up 2FA on all critical accounts, including email, banking, and internal systems.

Password Security Tips

- Be cautious of phishing emails asking for your password.
- Always log out of your accounts when using shared or public devices.
- Regularly review your account activity for unauthorized access.

Take Action Now!

Review your passwords today. Update them to meet security standards, and enable 2FA to add another layer of protection.

Reminder

For more information on cybersecurity best practices, visit the Australian Cyber Security Centre (ACSC) website or contact your IT security team.